REMARKS

Prior to a first Office Action, Applicant requests amendment of the Specification and Claims as set forth in this paper. Inasmuch as this application has yet to receive a first Office Action, the present amendment is not made to overcome any rejection of a claim or claims. Rather, upon a review of the application as filed, an amendment was made to further define Applicant's invention and to correct an erroneous reference in the Specification.

Favorable consideration of this application is respectfully requested.

A check in the amount of $126.00 is enclosed as fees for the added claims. Although no other fees are believed to be currently due, the Commissioner is hereby authorized to charge any other fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully Submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant

Harold E. Meier
Reg. No. 22,428

Correspondence Address:
2001 Ross Avenue, Suite 600
Dallas, Texas 75201-2980
214.953.6650
FAX: 214.661.4650

Date: October 17, 2001

MARKED-UP VERSION OF SPECIFICATION AND CLAIM AMENDMENTS

The Specification and Claims have been amended as follows:

IN THE SPECIFICATION:

Please replace the paragraph beginning on line 21 of page 10 with the following paragraph:

(Amended) In accordance with the present invention there is introduced the concept of Limited One-Way Functions, which are used to create computational terms barriers. The invention utilizes functions that are strongly asymmetric in nature, in terms of work to compute and work to invert. This class of functions, however, is not required to be completely intractable, but alternatively should have some measurable difference in the amount of work required to invert, compared to the cost of calculation of the output of the function. The application of this invention to key escrowing is described. A basic algorithm for implementation as an example of a suitable limited one-way function is described. This problem involves randomization and can be viewed as an extension of the puzzling problem originally developed by **[R. C. Merkle "Secure Communications Over an Insecure Channel," IEEE Trans. on Information Theory, 1976, IT-22, pages 644-654]** **Ralph C. Merkle, "Secure Communications Over Insecure Channels," Communications of the ACM, April 1978, Volume 21, Number 4, pages 294-299**. The basic algorithm utilized in implementation of the invention requires a randomized response and achieves a limited, but measurable computational advantage of the data receiver over an eavesdropper. Algorithm performance and application to the implementation of a delay function for employment in key escrow systems is hereinafter explained.

IN THE CLAIMS:

For the convenience of the Examiner, all pending claims are shown below whether or not an amendment has been made.

1. **(Amended)** A method for **storing and** withdrawing **[an encryption] a decryption** key from a key escrow database, comprising:

creating a set of N trap door encryption-decryption function pairs each paired with a corresponding token;

transmitting the set of N trap door encryption-decryption function pairs **along with a corresponding token** to a receiver;

randomly selecting at the receiver one of the trap door encryption-decryption function pairs and the **[paired] corresponding** token;

adding randomization information **at the receiver** to the **corresponding token of the** selected trap door encryption-decryption function pair **[and the corresponding token]**;

encrypting **the token with the added randomization information, [a decryption key using]** the **[corresponding]** token **corresponding** with the randomly selected encryption-decryption function pair;

recording **in a key escrow database** the created set of N trap door encryption-decryption function pairs and the corresponding paired token;

recording **in the key escrow database** the **[encrypted]** randomly selected trap door encryption-decryption function pair along with the **encrypted token [decryption key in a key escrow database]**; and

inverting the created set of N trap door encryption-decryption function pairs and the **[encrypted]** randomly selected trap door encryption-decryption function pair along with the **encrypted token [decryption key]** to identify the decryption key.

2. **(Amended)** A method for **storing and** withdrawing **[an encryption] a decryption** key from a key escrow database as in Claim 1, further comprising:

encrypting the created set of N trap door**[, the]** encryption-decryption function pairs and the randomly selected trap door function along with the decryption key prior to recording in **[an] the key** escrow database.

3. **(Amended)** The method for **storing and** withdrawing **[an encryption] a decryption** key from a key escrow database as in Claim 1, further comprising:

randomly selecting at the receiver an additional trap door encryption-decryption function pair and the **[paired] corresponding** token;

adding randomization information to the **corresponding token of the** additional selected trap door encryption-decryption function pair **[and the corresponding token]**;

concatenating the results of the adding of randomization information to the **corresponding token of the** additional selected trap door encryption-decryption function pair to the **[encryption of the] corresponding token of the** randomly selected first trap door encryption-decryption function pair; and

encrypting the concatenating results using the **[encryption] decryption** key from the **additional selected trap door encryption-decryption function pair [second choice]**.

4. **(Amended)** The method for **storing and** withdrawing **[an encryption] a decryption** key from a key escrow database as in Claim 1 further comprising adding signature information **at the receiver** to the selected trap door encryption-decryption function pair to distinguish valid subsequent decodings **of the selected trap door encryption-decryption function pair** from invalid decodings.

5. **(Amended)** The method for **storing and** withdrawing **[an encryption] a decryption** key from a key escrow database as in Claim 1, wherein encrypting **the corresponding token of** a selected trap door encryption-decryption function pair comprises calculating a cryptogram utilizing the corresponding token and including **[an encryption] a decryption** key along with randomization information**[, as well as additional] and signature** information **[added for signature purposes]**.

6. **(Amended)** A method for **storing and** withdrawing **[encryption] decryption** keys from a key escrow database, comprising:

generating, in accordance with a selected encryption function, a set of *N* cryptogram/decryption key pairs, each pair having a corresponding token;

transmitting the set of N cryptogram/decryption key pairs **and the corresponding token** to a receiver;

randomly selecting at the receiver one of the cryptogram/decryption key pairs along with the corresponding token;

decrypting the randomly selected cryptogram utilizing the corresponding token to obtain a corresponding **[encryption] decryption** key;

generating a cryptogram utilizing the corresponding **[encryption] decryption** key and comprising the selected token and randomization information;

recording in an escrow database the generated set of N cryptogram/decryption key pairs along with each corresponding token and the generated cryptogram based on the randomly selected cryptogram/decryption key pair; and

inverting the recorded set of N cryptogram/decryption key pairs and the generated cryptogram to identify **[an encryption] a decryption** key from the key escrow database.

7. **(Amended)** The method for **storing and** withdrawing **[encryption] decryption** keys from a key escrow database as in Claim 6, further comprising:

randomly selecting at the receiver one or more additional *N* cryptogram/decryption key pairs and corresponding tokens;

decrypting each cryptogram using the **[associated] corresponding** token of the additionally selected encryption/decryption key pairs to identify a corresponding **[encryption] decryption** key for each additionally selected pair;

generating a response cryptogram for each additionally selected cryptogram/decryption key pair utilizing the corresponding **[encryption] decryption** key and comprising the selected **additional** token**(s)** and randomization information; and

mixing the token information from one selected **key** pair with the response cryptogram from a different selected **key** pair along with randomization information to diffuse response structure prior to generating another response cryptogram.

8. **(Amended)** The method for **storing and** withdrawing **[encryption] decryption** keys from a key escrow database as in Claim **[6] 7**, further comprising:

decrypting the cryptogram of a cryptogram/decryption key pair using the associated decryption key to identify token information.

9. **(Amended)** The method for **storing and** withdrawing **[encryption] decryption** keys from a key escrow database as in Claim 8 wherein mixing comprises utilization of a linear transform.

10. The method for **storing and** withdrawing **[encryption] decryption** keys from a key escrow database as in Claim 8 wherein mixing comprises utilization of a symmetrical cryptosystem.

11. The method for **storing and** withdrawing **[encryption] decryption** keys from a key escrow database as in Claim 8 wherein mixing further comprises utilization of a public key cryptosystem.

12. The method for **storing and** withdrawing **[encryption] decryption** keys from a key escrow database as in Claim 6 wherein recording in an escrow database further comprises encrypting the generated set of N cryptogram/decryption key pairs and **[the] a** response message **from the receiver** prior to recording.

13. **(Amended)** The method for **storing and** withdrawing **[encryption] decryption** keys from a key escrow database as in Claim **[6] 12** further comprising adding signature information to the response message to enable valid decodings **of the response message** to be distinguished from invalid decodings.

14. **(Amended)** A method for secure communication between an originator and a receiver using message encryption, comprising:

creating at an originator a set of N trap door functions each paired with a corresponding token, each trap door function comprising a cryptogram/decryption key pair;

transmitting the set of N trap door functions to a receiver;

randomly selecting at the receiver one of the trap door functions and the **[paired]** **corresponding** token;

adding **at the receiver** randomization information to the corresponding token of the selected trap door function;

encrypting **at the receiver the decryption** **[an escrow]** key with the randomly selected trap door function;

transmitting the encrypted **decryption** key with the randomly selected trap door function to the originator; and

decoding the encrypted **[escrow]** **decryption** key with the randomly selected trap door function utilizing **originator** retained trap door information.

15. **(Amended)** The **[process]** **method** as in Claim 14 further comprising decrypting **at the receiver** the cryptogram to identify the corresponding token utilizing the decryption key of the cryptogram/decryption key pair.

16. **(Amended)** The method as in Claim 15 wherein encrypting **at the receiver** an escrow key comprises generating a cryptogram comprising the corresponding token, the decryption key and randomization information.

17. **(Amended)** The method **[of]** **as in** Claim 14 wherein decoding the encrypted **escrow** key comprises selecting a decryption key randomly from a selected group of decryption keys.

18. **(Amended)** The method **[of]** **as in** Claim 17 further comprising recognizing a correct decoding result utilizing structural information embedded in the response message.

19. **(Amended)** The method **[of]** **as in** Claim 14 wherein creating at an originator further comprises generating the set of N trap door functions utilizing a selected encryption function and a private encryption key.

Add the following new claims:

-- 20. (New) The method as in Claim 14 further comprising:

randomly selecting at the receiver an additional trap door function and the corresponding token;

adding randomization information to the corresponding token of the additional selected trap door function;

concatenating the results of the adding of the randomization information to the corresponding token of the additional selected trap door function to the encryption of the randomly selected first trap door function; and

encrypting the concatenating results using the decryption key from the additional selected trap door function pair.

21. (New) The method as in Claim 14 further comprising adding signature information at the receiver to the selected trap door function to distinguish valid subsequent decodings of the encrypted escrow key from invalid decodings.

22. (New) The method as in Claim 14 further comprising:

randomly selecting at the receiver one or more additional trap door functions and corresponding tokens;

decrypting each cryptogram of the selected trap door functions utilizing the corresponding token of the additionally selected trap door functions to identify the corresponding decryption key for each additionally selected pair;

adding at the receiver randomization information to the corresponding token of the additionally selected trap door functions;

encrypting at the receiver an escrow key for each of the additionally selected trap door functions utilizing the corresponding description key and comprising the selected additional tokens and randomization information; and

mixing the token information from one selected trap door function with the encryption from a different selected trap door function along with randomization information to diffuse response structure prior to encrypting another trap door function.

23. (New) The method as in Claim 22 wherein mixing comprises utilization of a symmetrical cryptosystem.

24. (New) The method as in Claim 22 wherein mixing further comprises utilization of a public key cryptosystem.

25. (New) The method as in Claim 22 wherein mixing comprises utilization of a symmetrical cryptosystem.

26. (New) The method as in Claim 14 further comprising recording in an escrow database the created N trap door functions along with each corresponding token and the encrypted escrow key with the randomly selected trap door function.

27. (New) The method as in Claim 26 further comprising inverting the recorded set of N trap door functions and the encrypted escrow key with the randomly selected trap door function to identify a decryption key from the key escrow database. --